Customer Responsibilities Guide

SecureEdge

April 2023

RESPONSIBILITIES GUIDE

RESPONSIBILITIES GUIDE

1.   ABOUT THIS GUIDE

There are a number of terms, conditions, requirements, roles and responsibilities associated with the purchase and use of SecureEdge services.

The guide outlines both your and our roles and responsibilities regarding each SecureEdge service

Requirements are split according to:

- SecureEdge (applies to all categories)
- SecureEdge Network
- SecureEdge Cloud
- SecureEdge Remote
- SecureEdge Connect
- SecureEdge Managed Service (SEMS)

This guide is the companion document to the SecureEdge section of Our Customer Terms, and your application form.

1.1 REQUIREMENTS

You are expected to manage and use your SecureEdge service according to the requirements outlined in this guide.

If you choose not to follow these requirements, we will not be responsible for any loss or inconvenience experienced if your SecureEdge service is disrupted. In this circumstance, we may charge you additional fees in order to fix your SecureEdge service.

You are required to provide us with all applicable information, data, consents, authorisations, decisions, and approvals in order to activate service requests.

You can make changes to your SecureEdge service using the User Interface.

It is your responsibility to identify any moves, additions or changes relevant to your SecureEdge service and submit the appropriate requests via the FNC portal request (fees applies).

You are also required to identify when you need assistance from your assigned Telstra account executive and submit the appropriate requests.

1.2 OUR REQUIREMENTS

We will provide the SecureEdge service according to the requirements outlined in this guide.

Our services are backed by service targets regarding availability, so you get the most out of your SecureEdge service.

We will provide service support, notify you of any service changes and let you know in writing when a service request has been completed.

RESPONSIBILITIES GUIDE

1.3 KEEPING YOUR CONTACT DETAILS UP-TO-DATE

From time-to-time we will need to get in contact with you regarding your SecureEdge service, so it's important that you keep your organisation's details up to date.

As a SecureEdge customer, you need to ensure that the following contact details are correct and kept up to date:

Commercial contact: the authorised staff member who acts on your business' behalf regarding all commercial matters associated with your SecureEdge service. <u>Note</u>: your Telstra account executive may call these contacts the 'primary contact' when buying SecureEdge services on your behalf.

Technical contact: the authorised person who answers any technical questions associated with your SecureEdge service on your behalf.

You can update your contact details via your Telstra account executive.

2. GENERAL SERVICE RESPONSIBILITIES

Various service activations and modification all have different responsibilities depending on the complexity of the action required. These responsibilities for the SecureEdge service are listed below within the table.

General Service Responsibilities

This section is applicable to all SecureEdge services.

RESPONSIBILITIES GUIDE

REQUIREMENT	RESPONSIBILITY	
	US	YOU
If you believe we have not satisfactorily completed a service or product installation, inform us within 5 business days of completion.		✓
Report any faults with your products through the Telstra SecureEdge User Interface or via the Telstra helpdesk.		✓
Provide updates on the progress of all reported faults within the relevant service target as set out in Our Customer Terms.	✓	
Request additional user login accounts for end-users on the SecureEdge User Interface.		✓
Create additional user login accounts for end-users on the SecureEdge User Interface.	✓	
Manage login accounts for end-users on the SecureEdge User Interface.		✓
Access and customise reports via the SecureEdge User Interface. For example, real time log and security event data and device policy.		✓
Advise Telstra of any changes to your contact details for notifications within 10 business days.		✓
Specify any network changes that may affect the device operational (if you own and manage the network yourself).		✓
Protect your log data and allow you to access this information via the SecureEdge User Interface.	✓	
Commence billing for the SecureEdge service after 5 business days from the handover of the SecureEdge service unless a fault has been identified and agreed to by us.	✓	
SERVICE ACTIVATION		
Provide a single point of contact for the activation of the SecureEdge service.	✓	✓
Plan your SecureEdge service deployment, including the collection and verification of information essential to the installation of your service.	✓	
Provide a network diagram and other relevant information upon request.		✓
Provide the required information specified within the application form.		✓
Provide support for the onboarding of the SecureEdge service that may include, but is not limited to: • access to technical teams • project support • change control approvals • organisation change communications		✓

RESPONSIBILITIES GUIDE

• management support.		
Apply the default policy to your SecureEdge service if applicable	✓	
Execute formal test plan in conjunction with you to test functionality and connectivity to your applications for final sign off	✓	✓
Prepare for transfer from the deployment team to SecureEdge operations team	✓	
Provide details for requesting Managed Services Support	✓	
Provide details of the SecureEdge User Interface	✓	
Complete all acceptance testing and provide signoff of the implemented design within 5 business days after the date of handover of the SecureEdge service.		✓
ONGOING		
Ensure your SecureEdge User Interface access credentials are not used to access or modify the SecureEdge service by any parties other than Telstra or partners authorised by Telstra for the management of SecureEdge.		✓
Raise an FNC request to make policy or routing changes		✓
Provide maintenance period options if a network outage is expected, during which time Telstra specialists will examine and maintain SecureEdge service	✓	
Select a maintenance period provided by Telstra for your SecureEdge service when required		✓
Ensure the configuration you implement to your SecureEdge service does not prevent us from managing the SecureEdge service	✓	
SERVICE CANCELLATION		
Within 30 days prior to cancelling your service, inform us in writing if you wish to extract your logs		✓

RESPONSIBILITIES GUIDE

3. SEMS SERVICE RESPONSIBILITIES

This section is applicable to SecureEdge Managed Service (SEMS).

REQUIREMENT	RESPONSIBILITY	
	US	YOU
If you believe we have not satisfactorily completed a SEMs request, inform us within 2 business days of completion.		✓
Provide an access method to submit SEMS requests	✓	
Provide sufficient details for the SEMS request to be executed successfully		✓
Accept a read only access to the SecureEdge User Interface while SEMS is operational		✓
Agree with Telstra if you need edit access to the SecureEdge User Interface while SEMS is operational		✓

RESPONSIBILITIES GUIDE

4. SERVICE TARGETS

The various targets for service activations and modifications all have different corresponding timelines depending on the complexity of the action required.

These timelines can also be affected by factors such as volume. For example, creating a simple policy rule on single appliance is a relatively minor piece of work, while creating complex policy rule across multiple security appliances can take an additional amount of time.

SecureEdge Managed Service (SEMS)

REQUIREMENT	RESPONSIBILITY	
	US	YOU
SERVICE MODIFICATIONS		
MINOR Request to reset a password Request to have user created Change a Security Contact		✓
MAJOR Cancel a service Relocate a service from one physical location to another location Upgrade or downgrade from one management tier to another management tier		✓